UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/026,813	12/27/2001	Hiroo Nakano	217781US2S	1908

22850 7590 05/16/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
ALOMARI, FIRAS B	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/026,813	NAKANO, HIROO	
	Examiner	Art Unit	
	Firas Alomari	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/7/03, 5/12/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-5, 8, 11-15 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ugon et al US (6,839,849) in view of Feyt et al. US (6,698,662).

Regarding claims 1, 3, 11 and 13: Ugon discloses a data processing apparatus comprising:

An operation processing unit (FIG.1 item 1) having at least a read cycle period when said operation processing unit reads data from a device (Col 5, Lines 65-67), and a write cycle period when said operation processing unit writes data in the device (Col 6, Lines 2-5); a memory which performs data transmission/reception between said operation processing unit and said memory;(Col 5, Lines 62-65 and Col 6, Lines 12-17) a data bus connected to said operation processing unit and said memory;(Col 5, Lines 3-10) and a pseudo-data generating circuit connected to said data bus,(Col 11, Lines 14-18) said pseudo-data generating circuit which generates pseudo-data and outputs

the pseudo-data to said memory to cause instruction to randomly execute (Col 11, lines 22-25) but he doesn't explicitly disclose the pseudo-data generating circuit outputs the pseudo-data to said data bus in a time interval between the read cycle period and the write cycle period, between the write cycle period and the read cycle period, between two read cycle periods, or between two write cycle periods. However Feyt et al. discloses a method for hiding operation performed by microprocessor card where he teaches presenting a random data items on the data bus during cryptographic calculation like read and write operations (Col 2, Lines 36-42 and Col 3, Lines 34-52). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the Ugon system with the teaching of Feyt to output pseudo-data on the data bus between read and write cycles. One would be motivated to do so in order to mask the power consumption by the memory during the reading or writing of secret data to prevent an attacker from deducing the data by correlation or differential power analysis attacks. (Col 1, lines 36-46)

Regarding claims 2,4,12 and 14: Ugon discloses the data processing apparatus according to claim 1, wherein said pseudo-data generating circuit generates random number data as the pseudo-data. (Col 11, Lines 14-18 and Col 12, lines 34-37)

Regarding claims 5,8,15 and 18: Ugon discloses a data processing apparatus comprising:

an operation processing unit (FIG.1 item 1) having at least a read cycle period when said operation processing unit reads data from a device, (Col 5, Lines 65-67) and a write cycle period when said operation processing unit writes data in the device(Col 6, Lines 2-5); a memory which performs data transmission/reception between said operation processing unit and said memory; (Col 5, Lines 62-65 and Col 6, Lines 12-17) a data bus connected to said operation processing unit and said memory(Col 5, Lines 3-10); and a dummy circuit connected to said data bus,(Col 5, Lines 10-13) said dummy circuit operates and consumes power (Col 11, Lines 9-11) but he doesn't explicitly disclose the dummy circuit operates and consumes power in a time interval between the read cycle period and the write cycle period, between the write cycle period and the read cycle period, between two read cycle periods, or between two write cycle periods. However Feyt et al. discloses a method for hiding operation performed by microprocessor card where he teaches masking cryptographic calculation thorough writing random data in a reserved memory location between the reading or writing of cryptographic information using transistors that are powered according to random signal to make the total power consumption random through the operation (Col 2, Lines 57-6 and Col 3, Lines 49-54). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the Ugon system with the teaching of Feyt to include a circuit that consumes power between read and write cycles. One would be motivated to do so in order to mask the power consumption during the reading or writing of secret data by adding random additional power

consumption to the normal power consumption modifying the total value and hiding the power consumption resulting from the cryptographic operations. (Col 2, lines 48-52)

3. Claims 6-7, 9-10, 16-17 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ugon et al US (6,839,849) in view of Feyt et al. US (6,698,662) as applied to claims 1-5, 8, 11-15 and 18 above, and further in view of Schneier B, Applied Cryptography, 1996, 2nd Edition, P197-206 and P372-375.

Regarding claims 6, 9, 16 and 19: The combination of Ugon and Feyt doesn't explicitly disclose the data processing apparatus according to claim 5, wherein said dummy circuit is a counter circuit. However Schneier teaches a stream cipher encryption/decryption method where he uses a running-key generator comprising a counter register that outputs a stream of bits within the stream of plain text to produce the cipher text (Page 205, Paragraph 5 and Page 197, Paragraph 3). Therefore it would have been to one ordinary skilled in the art at the time the invention was made to modify the combination of Ugon and Feyt with the teachings of Schneier to include a counter circuit in the dummy circuit because counter circuits are easily implemented in hardware (Page 373, Paragraph 2) additionally counter circuits are widely used in cryptographic processors therefore the dummy circuit and the processor will have similar power

consumption making the correlation and differential power analysis attacks on the system harder.

Regarding claims 7, 10, 17 and 20: The combination of Ugon and Feyt doesn't explicitly disclose the data processing apparatus according to claim 5, wherein said dummy circuit is a shift register circuit. However Schneier teaches a stream cipher encryption/decryption method where he uses a running-key generator comprising a shift register that outputs a stream of bits within the stream of plain text to produce the cipher text (Page 206, Paragraph and Page 197, Paragraph 3). Therefore it would have been to one ordinary skilled in the art at the time the invention was made to modify the combination of Ugon and Feyt with the teachings of Schneier to include a shift register circuit in the dummy circuit because shift register circuits are easily implemented in hardware (Page 373, Paragraph 2) additionally shift register circuits are widely used in cryptographic processors therefore the dummy circuit and the processor will have similar power consumption making the correlation and differential power analysis attacks on the system harder.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached on M-F from 7:30 am - 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari
Examiner
Art Unit 2136

FA

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100